

Amendment and Response Under 37 C.F.R. 1.116

Applicant: Kevin R. Driscoll

Serial No.: 09/712,505

Filed: November 14, 2000

Docket No.: H16-26353 (H162.104.101)

Title: CRYPTOGRAPHIC COMBINER USING TWO SEQUENTIAL NON-ASSOCIATIVE OPERATIONS

IN THE CLAIMS

1. (Original) A stream cipher cryptosystem comprising:
a source for providing an encryption keystream;
an encryption combiner receiving a first plaintext binary data sequence and the encryption keystream and performing a first set of two non-associative operations on the first plaintext binary data sequence and the encryption keystream to provide a ciphertext binary data sequence;
a source for providing a decryption keystream; and
a decryption combiner receiving the ciphertext binary data sequence and the decryption keystream and performing a second set of two non-associative operations on the ciphertext binary data sequence and the decryption keystream to provide a second plaintext binary data sequence substantially similar to the first plaintext binary data sequence.
2. (Original) The stream cipher cryptosystem of claim 1 wherein each operation in the second set is the inverse of an operation in the first set.
3. (Original) The stream cipher cryptosystem of claim 1 wherein the operations in the first set include an integer addition operation and an XOR operation, and the operations in the second set include an integer subtraction operation and an XOR operation.
4. (Original) The stream cipher cryptosystem of claim 1 wherein the operations in the first set include an integer subtraction operation and an XOR operation, and the operations in the second set include an integer addition operation and an XOR operation.
5. (Original) The stream cipher cryptosystem of claim 1 wherein the operations in the first set include a modular multiplication operation and an XOR operation, and the operations in the second set include an inverse modular multiplication operation and an XOR operation.

Amendment and Response Under 37 C.F.R. 1.116

Applicant: Kevin R. Driscoll

Serial No.: 09/712,505

Filed: November 14, 2000

Docket No.: H16-26353 (H162.104.101)

Title: CRYPTOGRAPHIC COMBINER USING TWO SEQUENTIAL NON-ASSOCIATIVE OPERATIONS

6. (Original) The stream cipher cryptosystem of claim 1 wherein the operations in the first set include an inverse modular multiplication operation and an XOR operation, and the operations in the second set include a modular multiplication operation and an XOR operation.

7. (Original) The stream cipher cryptosystem of claim 1 wherein the operations in the first set include a rotate right operation and an XOR operation, and the operations in the second set include a rotate left operation and an XOR operation.

8. (Original) The stream cipher cryptosystem of claim 1 wherein the operations in the first set include a rotate left operation and an XOR operation, and the operations in the second set include a rotate right operation and an XOR operation.

9. (Original) A stream cipher cryptosystem comprising:
a source for receiving a key and providing a keystream; and
a cryptographic combiner receiving a first binary data sequence and the keystream and performing two sequential non-associative operations on the first binary data sequence and the keystream to provide a second binary data sequence.

10. (Original) The stream cipher cryptosystem of claim 9 wherein the cryptographic combiner is an encryption combiner and the first binary data sequence is a plaintext binary data sequence and the second binary data sequence is a ciphertext binary data sequence.

11. (Original) The stream cipher cryptosystem of claim 9 wherein the cryptographic combiner is a decryption combiner and the first binary data sequence is a ciphertext binary data sequence and the second binary data sequence is a plaintext binary data sequence.

12. (Original) The stream cipher cryptosystem of claim 9 wherein the two sequential non-associative operations are an integer addition operation and an XOR operation.

Amendment and Response Under 37 C.F.R. 1.116

Applicant: Kevin R. Driscoll

Serial No.: 09/712,505

Filed: November 14, 2000

Docket No.: H16-26353 (H162.104.101)

Title: CRYPTOGRAPHIC COMBINER USING TWO SEQUENTIAL NON-ASSOCIATIVE OPERATIONS

13. (Original) The stream cipher cryptosystem of claim 9 wherein the two sequential non-associative operations are an integer subtraction operation and an XOR operation.

14. (Original) The stream cipher cryptosystem of claim 9 wherein the two sequential non-associative operations are a modular multiplication operation and an XOR operation.

15. (Original) The stream cipher cryptosystem of claim 9 wherein the two sequential non-associative operations are an inverse modular multiplication operation and an XOR operation.

16. (Original) The stream cipher cryptosystem of claim 9 wherein the two sequential non-associative operations are a rotate right operation and an XOR operation.

17. (Original) The stream cipher cryptosystem of claim 9 wherein the two sequential non-associative operations are a rotate left operation and an XOR operation.

18. (Original) A method of encrypting a plaintext binary data sequence, the method comprising the steps of:

generating an encryption keystream as a function of a key; and
combining the plaintext binary data sequence and the encryption keystream with two non-associative operations to provide a ciphertext binary data sequence.

19. (Original) The method of claim 18 wherein the two non-associative operations include an integer addition operation.

20. (Original) The method of claim 19 wherein the two non-associative operations include an XOR operation.

Amendment and Response Under 37 C.F.R. 1.116

Applicant: Kevin R. Driscoll

Serial No.: 09/712,505

Filed: November 14, 2000

Docket No.: H16-26353 (H162.104.101)

Title: CRYPTOGRAPHIC COMBINER USING TWO SEQUENTIAL NON-ASSOCIATIVE OPERATIONS

21. (Original) The method of claim 18 wherein the two non-associative operations include an integer subtraction operation.
22. (Original) The method of claim 21 wherein the two non-associative operations include an XOR operation.
23. (Original) The method of claim 18 wherein the two non-associative operations include a modular multiplication operation.
24. (Original) The method of claim 23 wherein the two non-associative operations include an XOR operation.
25. (Original) The method of claim 18 wherein the two non-associative operations include an inverse modular multiplication operation.
26. (Original) The method of claim 25 wherein the two non-associative operations include an XOR operation.
27. (Original) The method of claim 18 wherein the two non-associative operations include a rotate right operation.
28. (Original) The method of claim 27 wherein the two non-associative operations include an XOR operation.
29. (Original) The method of claim 18 wherein the two non-associative operations include a rotate left operation.
30. (Original) The method of claim 29 wherein the two non-associative operations include an XOR operation.

Amendment and Response Under 37 C.F.R. 1.116

Applicant: Kevin R. Driscoll

Serial No.: 09/712,505

Filed: November 14, 2000

Docket No.: H16-26353 (H162.104.101)

Title: CRYPTOGRAPHIC COMBINER USING TWO SEQUENTIAL NON-ASSOCIATIVE OPERATIONS

31. (Original) A method of decrypting a ciphertext binary data sequence, the method comprising the steps of:

generating a decryption keystream as a function of a key; and

combining the ciphertext binary data sequence and the decryption keystream with two non-associative operations to provide a plaintext binary data sequence.

32. (Original) The method of claim 31 wherein the two non-associative operations include an integer addition operation.

33. (Original) The method of claim 32 wherein the two non-associative operations include an XOR operation.

34. (Original) The method of claim 31 wherein the two non-associative operations include an integer subtraction operation.

35. (Original) The method of claim 34 wherein the two non-associative operations include an XOR operation.

36. (Original) The method of claim 31 wherein the two non-associative operations include a modular multiplication operation.

37. (Original) The method of claim 36 wherein the two non-associative operations include an XOR operation.

38. (Original) The method of claim 31 wherein the two non-associative operations include an inverse modular multiplication operation.

Amendment and Response Under 37 C.F.R. 1.116

Applicant: Kevin R. Driscoll

Serial No.: 09/712,505

Filed: November 14, 2000

Docket No.: H16-26353 (H162.104.101)

Title: CRYPTOGRAPHIC COMBINER USING TWO SEQUENTIAL NON-ASSOCIATIVE OPERATIONS

39. (Original) The method of claim 38 wherein the two non-associative operations include an XOR operation.
40. (Original) The method of claim 31 wherein the two non-associative operations include a rotate right operation.
41. (Original) The method of claim 40 wherein the two non-associative operations include an XOR operation.
42. (Original) The method of claim 31 wherein the two non-associative operations include a rotate left operation.
43. (Original) The method of claim 42 wherein the two non-associative operations include an XOR operation.